GANZ EINFACH

KRYPTO

Das Fundament deiner Souveränität.
Dein Imperium auf deiner Cloud.



Danilo Sieren

Danilo Sieren

Ganz Einfach

Krypto

Bitcoin und Kryptowerte verstehen
Wallets und digitales Erbe sicher verwalten

Überarbeitete und erweiterte
Neuauflage 2026

Vorwort

Kryptowerte zu verstehen bedeutet, technische Möglichkeiten und ihre Grenzen gemeinsam zu betrachten. Eine selbst verwaltete Wallet kann dir die Verfügung über digitale Werte geben. Sie nimmt dir aber weder das Kursrisiko noch die Verantwortung für Sicherung, Übertragung und Nachlass ab. Eine falsche Empfängeradresse oder ein offengelegtes Backup lässt sich häufig nicht durch einen Kundendienst korrigieren.

Dieses Buch führt dich von den Grundlagen bis zu einem dokumentierten, wiederherstellbaren Aufbau. Bitcoin bildet den technischen Schwerpunkt. Ethereum, Token, Stablecoins und Lightning werden dort ergänzt, wo andere Modelle andere Prüfungen verlangen. Du lernst, was eine Wallet tatsächlich speichert, wie du eine Transaktion kontrollierst und welche Informationen deine Angehörigen im Notfall benötigen.

Du brauchst zu Beginn weder einen Server noch eigenes Kryptovermögen. Die ersten Entscheidungen und Übungen lassen sich auf Papier oder in einer isolierten Testumgebung durchführen. Ein funktionierender Lernaufbau ist ein gutes Ergebnis. Daraus folgt keine Verpflichtung, anschließend Geld zu investieren.

Die Neuauflage trennt Netzwerksicherheit, Gerätesicherheit, Verwahrungsrisiken und rechtliche Fragen. Sie behandelt Privatsphäre als begrenzbare Datenweitergabe. Weder ein VPN noch Tor, Coinjoin oder eine eigene Node können vollständige Anonymität garantieren. Ebenso wenig garantiert eine Zulassung die Werthaltigkeit eines Tokens.

Der Quellenstand ist der 2. November 2026. Die technischen Kapitel beziehen sich auf die verlinkten offiziellen Projektunterlagen. Bei deutschen Steuerfragen werden geltende Vorschriften und das BMF-Schreiben vom März 2025 vom im September 2026 veröffentlichten Reformvorhaben unterschieden. Ein Referentenentwurf ist kein geltendes Gesetz. Für eine konkrete Erklärung zählt die im betreffenden Zeitraum wirksame Rechtslage.

So arbeitest du mit diesem Buch

Lies zuerst die Grundlagen und das Kapitel über deinen eigenen Bedarf. Danach folgen Schlüssel, Sicherungen und eine einfache Wallet. Erst wenn du einen Wiederherstellungsweg verstanden und mit einem kleinen Übungsbestand erprobt hast, sind Multisig oder eine eigene Serverinfrastruktur sinnvoll. Komplexität muss einen konkreten Vorteil bringen.

Die Praxisbeispiele verwenden erfundene Personen, Beträge und Vorgänge. Befehle für den Regtest erzeugen ausschließlich lokale Testwerte. Im Buch stehen keine produktiven Wiederherstellungswörter, privaten Schlüssel oder Zahlungsadressen. Platzhalter wie EMPFAENGER oder TXID musst du im passenden Zusammenhang ersetzen; sie sind keine ausführbaren Werte.

Einige Programmoberflächen sind auf Englisch dokumentiert. Begriffe wie Settings, Receive oder Send werden deshalb mit ihrer Aufgabe erklärt. Kontrolliere vor einem produktiven Einsatz die Dokumentation deiner installierten Version. Insbesondere Gerätefunktionen, unterstützte Netzwerke und Wiederherstellungsstandards können sich zwischen Modellen desselben Herstellers unterscheiden.

Technisches Verstehen ersetzt keine persönliche Anlage-, Steuer- oder Rechtsberatung. Dieses Buch empfiehlt keinen Kauf und keine bestimmte Gewichtung deines Vermögens. Bei Eigentumsstreitigkeiten, grenzüberschreitenden Sachverhalten, größeren Verlusten oder einem Nachlass brauchst du zusätzlich fachkundige Unterstützung. Die vorbereiteten Unterlagen helfen dir, diese Unterstützung gezielt in Anspruch zu nehmen.

Inhalt

Vorwort 2
So arbeitest du mit diesem Buch 4
1 Kryptowerte und deinen eigenen Bedarf verstehen 7
2 Bitcoin und andere Netzwerke sachlich einordnen 11
3 Schlüssel und Wallets verstehen 15
4 Wiederherstellungswörter und Passphrasen sichern 19
5 Sicherungsmedien und Aufbewahrung planen 23
6 Hardware und Software bewusst auswählen 27
7 Eine einfache Wallet kontrolliert einrichten 31
8 Bitcoin Transaktionen vollständig prüfen 35
9 UTXOs Gebühren und festhängende Zahlungen verwalten 39
10 Eine eigene Bitcoin Node sinnvoll planen 43
11 Bitcoin Core installieren und kontrollieren 47
12 Sparrow mit der eigenen Node verbinden 51
13 Multisig und geteilte Verantwortung planen 56
14 Eine Multisig Wallet nachvollziehbar einrichten 60
15 Wiederherstellung und Geräteverlust beherrschen 64
16 Kauf Verkauf und Verwahrung prüfen 68
17 Ethereum Token und Vertragsfreigaben verstehen 72
18 Stablecoins DeFi Staking und Brücken beurteilen 76
19 Privatsphäre auf der Blockchain realistisch beurteilen 80
20 Netzwerk und Rechner sinnvoll abschirmen 84
21 Lightning für kleine Zahlungen verstehen 88
22 Zahlungen mit BTCPay Server organisieren 92
23 Betrugsversuche und Fehlfreigaben erkennen 96
24 Bei einem Sicherheitsvorfall richtig reagieren 100
25 Regulierung und Pflichten in der EU einordnen 104

26 Deutsche Steuerfragen nach Zeitraum und Vorgang ordnen ... 108
27 Belege und Transaktionsdaten dauerhaft führen ... 112
28 Das digitale Erbe zugänglich und geschützt gestalten ... 116
29 Wartung und Änderungen kontrollieren ... 120
30 Langfristige Risiken und technische Entwicklung beurteilen ... 124
31 Entscheidungen unter Unsicherheit treffen ... 128
32 Einen vollständigen privaten Aufbau entwickeln ... 132
33 Bitcoin ohne echtes Geld im Regtest üben ... 136
34 Fehler nach ihrer tatsächlichen Ursache eingrenzen ... 141
A Lernwerkstatt mit überprüfbaren Aufgaben ... 145
B Fallwerkstätten für schwierige Situationen ... 153
C Abnahme eines konkreten Aufbaus ... 163
D Ein vollständiges Belegbeispiel durchrechnen ... 170
E Begriffe verständlich nachschlagen ... 178
F Vorlagen für Betrieb und Nachlass ... 186
G Vertiefende Prüfungen für fortgeschrittene Leser ... 192
H Eine Wallet Migration kontrolliert durchführen ... 198
Ausführlicher Inhalt ... 205
Stichwortverzeichnis ... 215
Quellen und weiterführende Dokumentation ... 222
Impressum ... 227

1 Kryptowerte und deinen eigenen Bedarf verstehen

1.1 Eine technische Möglichkeit von einem Anlageziel trennen

Beginne mit der Frage, welche Aufgabe du lösen möchtest. Vielleicht willst du eine Zahlung nachvollziehen, eine Wallet sicher bedienen oder einen vorhandenen Bestand für den Notfall dokumentieren. Diese Ziele lassen sich prüfen. Die Erwartung, mit Kryptowerten automatisch unabhängiger oder wohlhabender zu werden, ist dagegen keine technische Anforderung.

Kryptowerte können stark im Preis schwanken. Ein funktionierendes Netzwerk und eine korrekt verwahrte Wallet verhindern keinen wirtschaftlichen Verlust. Auch ein knappes Angebot begründet keinen bestimmten Marktpreis. Nachfrage, Liquidität, rechtliche Rahmenbedingungen und die Bereitschaft anderer Marktteilnehmer beeinflussen den Wert.

Trenne deshalb Lernbudget, laufende Ausgaben und langfristige Verpflichtungen. Geld für Miete, absehbare Rechnungen oder eine notwendige Rücklage ist kein geeigneter Übungsbestand. Wenn du eine technische Übertragung mit echtem Wert ausprobieren möchtest, lege zuerst einen Betrag fest, dessen vollständigen Verlust du tragen kannst. Diese Grenze folgt deiner Situation und keinem Prozentsatz aus einem Buch.

Schreibe deinen Zweck in einem Satz auf. Ein brauchbares Beispiel lautet: „Ich möchte einen kleinen bestehenden Bitcoin-Bestand so verwahren, dass ich eine Wiederherstellung erklären und durchführen kann.“ Anschließend ergänzst du, wer Zugang benötigt, welche Geräte verfügbar sind und wie viel Wartung du tatsächlich übernehmen willst.

1.2 Forderungen und eigene Schlüssel unterscheiden

Bei einem Bankguthaben hast du eine Forderung gegen das Institut. Dieser rechtliche Anspruch steht in einem geregelten Umfeld mit Aufsicht und gegebenenfalls Sicherungssystemen. Bei einem zentralen Kryptodienst kann ebenfalls eine Forderungs- oder Verwahrungsbeziehung bestehen. Entscheidend sind Vertrag, Rechtsordnung und tatsächliche Organisation des Dienstes.

Bei einer selbst verwalteten Bitcoin-Wallet kannst du gültige Transaktionen mit deinen Schlüsseln autorisieren. Das bedeutet technische Verfügungsmacht. Es bedeutet nicht automatisch, dass jede Ausgabe rechtlich erlaubt ist oder dass ein Streit über das Eigentum verschwindet. Ein gestohlener Schlüssel kann technisch funktionieren, obwohl sein Benutzer nicht berechtigt ist.

Eine zentrale Plattform kann Zugang sperren, Auszahlungen verzögern oder ausfallen. Selbstverwahrung verlagert einen Teil dieser Risiken auf dich: Du kannst ein Backup verlieren, eine schädliche Freigabe erteilen oder die falsche Kette verwenden. Die Wahl lautet deshalb nicht schlicht sicher oder unsicher. Du entscheidest, welche Risiken du selbst beherrschen kannst.

1.3 Coins und Token einordnen

Bitcoin ist der native Vermögenswert des Bitcoin-Netzwerks. Ether erfüllt diese Rolle bei Ethereum und dient dort unter anderem zur Bezahlung von Ausführungskosten. Ein Token kann auf einer bestehenden Blockchain durch einen Smart Contract verwaltet werden. Name und Symbol allein identifizieren ihn nicht zuverlässig.

Mehrere Token können denselben Namen tragen. Ein Euro- oder Dollarsymbol beweist weder eine Reserve noch einen einlösbaren Anspruch. Auch eine technisch übertragbare Einheit muss wirtschaftlich nicht liquide sein. Um einen konkreten Token zu bestimmen, benötigst du mindestens Netzwerk und gegebenenfalls die geprüfte Vertragsadresse aus einer verlässlichen Quelle.

Eine identisch aussehende Adresse auf zwei kompatiblen Netzwerken bedeutet nicht, dass eine Plattform Einzahlungen auf beiden akzeptiert. Wer nur das Symbol ETH oder USDC vergleicht, prüft den Vorgang unvollständig. Später übst du deshalb eine Übertragung als Kombination aus Vermögenswert, Netzwerk, Empfänger und gegebenenfalls Zusatzkennung.

1.4 Deine Grenzen schriftlich festlegen

Dein Betriebsprofil enthält mehr als eine Verlustgrenze. Halte fest, ob ein Angehöriger im Notfall handeln können soll, ob du häufig reist und ob du die Infrastruktur allein wartest. Eine komplizierte Mehrparteienlösung kann für einen kleinen Lernbestand ungeeignet sein, während eine einzige ungesicherte Mobiltelefon-Wallet für einen wichtigen Nachlass nicht ausreicht.

Ergänze klare Ausschlüsse: kein Kredit für Käufe, keine Freigabe während eines unerwarteten Anrufs, kein Wiederherstellungswort in einem Chat und keine neue Technik unmittelbar vor einer notwendigen Zahlung. Solche Regeln reduzieren Entscheidungen unter Zeitdruck.

Überprüfe das Profil nach wesentlichen Veränderungen. Ein Umzug, eine neue Vertrauensperson oder eine längere Krankheit kann die Aufbewahrung wichtiger machen als ein neues Gerätefeature. Die geeignete Lösung passt zu deinem Alltag und zu den Menschen, die sie später verstehen müssen.

1.5 Eine Entscheidung auch ohne Kauf abschließen

Ein technisches Lernprojekt kann mit der begründeten Entscheidung enden, vorerst keinen Bestand zu erwerben. Prüfe dafür die noch offenen Abhängigkeiten: Kannst du eine Sicherung schützen, einen Verlust tragen und den Zugang vertreten lassen? Wenn eine dieser Voraussetzungen fehlt, ist eine Pause ein sinnvolles Ergebnis.

Ein dokumentierter Lernfortschritt bleibt trotzdem nutzbar. Du kannst später an einem geprüften Punkt fortsetzen, statt unter neuem Marktdruck wieder bei null zu beginnen. Halte den nächsten notwendigen Schritt fest und vermeide einen bloßen Erinnerungsvermerk, irgendwann mehr zu recherchieren.

2 Bitcoin und andere Netzwerke sachlich einordnen

2.1 Was eine Blockchain tatsächlich leistet

Eine Blockchain ordnet Transaktionen in einer überprüfbaren Folge von Blöcken. Bei Bitcoin verweisen Blöcke auf Vorgänger und enthalten einen Nachweis geleisteter Arbeit. Die Teilnehmer prüfen Regeln wie Signaturen, Ausgabeberechtigungen und die zulässige Erzeugung neuer Einheiten. Das ursprüngliche Whitepaper beschreibt das Grundproblem konkurrierender Ausgaben und die Verkettung von Arbeitsnachweisen. [D01]

Ein gespeicherter Datensatz ist dadurch nicht automatisch wahr. Eine Blockchain kann dokumentieren, dass ein Schlüssel eine bestimmte Nachricht autorisiert hat. Sie bestätigt nicht ohne weitere Informationen, wem der Schlüssel rechtlich gehört oder ob eine gelieferte Ware den versprochenen Zustand hat.

Auch die Dauerhaftigkeit ist eine Systemeigenschaft mit Voraussetzungen. Software, Kommunikation, ökonomische Anreize und genügend unabhängige Teilnehmer müssen fortbestehen. Ein einzelner abgeschalteter Rechner löscht das Netzwerk nicht. Umgekehrt reicht die bloße Existenz irgendeiner alten Kopie nicht für einen weiterhin nutzbaren Markt.

2.2 Miner und prüfende Nodes auseinanderhalten

Miner stellen mögliche neue Bitcoin-Blöcke zusammen und suchen einen passenden Arbeitsnachweis. Vollständig prüfende Nodes entscheiden anhand ihrer installierten Regeln, welche Blöcke sie akzeptieren. Eine Node erhält durch ihre Anzahl allein keine proportionale Stimme wie bei einer Personenabstimmung.

Ein Miner kann keinen beliebigen fremden Bestand ausgeben, nur weil er viel Rechenleistung besitzt. Dazu wären weiterhin gültige Ausgabebedingungen zu erfüllen. Eine hohe Kontrolle über die Blockproduktion kann aber etwa Zensur und Umorganisationen begünstigen. Die häufige Behauptung, eine Mehrheit der Rechenleistung erlaube jede denkbare Manipulation, verwechselt verschiedene Angriffe.

Für dich als Nutzer zählt vor allem, welche Regeln deine Software prüft und von welcher Datenquelle deine Wallet ihre Sicht erhält. Eine eigene Node kann die Abhängigkeit von einem fremden Auskunftsdienst reduzieren. Sie ist keine Garantie gegen Malware auf deinem Rechner oder eine falsch bestätigte Empfängeradresse.

2.3 Bestätigungen und Finalität verstehen

Eine Bitcoin-Transaktion wird zunächst an erreichbare Teilnehmer weitergegeben. Jeder Teilnehmer besitzt seine eigene Sicht auf unbestätigte Vorgänge. Einen zentralen, weltweit identischen Mempool gibt es nicht. Ein Eintrag in einem öffentlichen Explorer ist daher keine Zusicherung einer späteren Bestätigung.

Nach Aufnahme in einen akzeptierten Block erhält die Transaktion eine Bestätigung. Weitere Blöcke erhöhen den Aufwand einer möglichen Umorganisation. Das ist probabilistische Absicherung. Eine feste Zahl wie sechs Bestätigungen ist eine verbreitete Konvention für manche Anwendungen, aber keine Naturkonstante für jeden Betrag und jedes Risiko.

Ethereum verwendet einen anderen Konsens mit Validatoren und Proof of Stake. Dort sind Blockvorschlag, Bestätigungen und protokollseitige Finalität anders organisiert. Eine Anzeige von mehreren Bestätigungen darf deshalb nicht ungeprüft zwischen Netzwerken gleichgesetzt werden. Auch bei finalisierten Transaktionen bleiben Fehler im Empfänger, im Vertrag oder in einer zusätzlichen Brücke möglich. [D29]

2.4 Knappheit und Änderungen der Regeln unterscheiden

Die bekannten Bitcoin-Regeln begrenzen die Gesamtausgabe durch die abnehmende Blocksubvention. Diese Regel ist in Software implementiert und wird von Teilnehmern durchgesetzt. Sie ist kein physikalisches Gesetz, das unabhängig von jeder sozialen Entscheidung existiert.

Teilnehmer können Software verändern. Ob eine Änderung angenommen wird und welche Kette wirtschaftlich als Bitcoin behandelt wird, hängt von der tatsächlichen Nutzung ab. Eine Änderung durch einen einzelnen Entwickler verpflichtet nicht alle anderen. Ebenso garantiert der Betrieb deiner eigenen Node nicht, dass du einen großen Markt von einer abweichenden Regel überzeugst.

Bei einer Spaltung können verschiedene Netzwerke mit gemeinsamer Vorgeschichte entstehen. Daraus folgt kein risikoloser Zusatzgewinn. Das Einlösen vermeintlich neuer Ansprüche kann Schlüssel offenlegen oder Wiederholungen von Transaktionen ermöglichen. Bewahre bei einer solchen Situation zunächst deinen unveränderten Sicherungsstand und prüfe projektspezifische Hinweise.

2.5 Energieverbrauch ohne einfache Gleichsetzung betrachten

Proof of Work benötigt Energie für die Blockproduktion. Dein normaler Rechner wird dadurch nicht automatisch zu einem wirtschaftlich sinnvollen Bitcoin-Miner. Spezialhardware, Stromkosten, Kühlung und Wettbewerb beeinflussen die Rechnung. Eine Full Node zu betreiben ist eine andere Aufgabe als Mining.

Ein pauschaler Stromwert pro einzelner Zahlung beschreibt das System nur eingeschränkt. Blockproduktion und Netzwerksicherheit laufen unabhängig von deiner konkreten Übertragung, während zusätzliche Schichten weitere Zahlungen bündeln können. Daraus folgt aber nicht, dass der Energieverbrauch bedeutungslos wäre.

Für deinen eigenen Aufbau kannst du reale Leistungsaufnahme und Betriebszeit messen. Ein nur gelegentlich benötigtes Testsystem muss nicht dauerhaft laufen. Bei einer ständig betriebenen Node gehören Strom, Datenspeicher und Wartung zur Entscheidung. Wirtschaftliche und ökologische Bewertungen sollten ihre Messgrenzen offenlegen.

2.6 Eine Blockchain Aussage an ihrem Umfang prüfen

Die Aussage „Die Transaktion ist bestätigt“ beschreibt einen technischen Zustand. Sie beantwortet nicht, ob der richtige Mensch bezahlt wurde, ob eine Ware geliefert wurde oder ob die Zahlung steuerlich vollständig dokumentiert ist. Schreibe diese Ebenen getrennt auf.

Dasselbe gilt für Dezentralität. Ein Netzwerk kann viele prüfende Teilnehmer besitzen, während deine konkrete Nutzung von einer einzigen Börse, einem einzelnen Webfrontend oder einer bestimmten Hardwarelieferkette abhängt. Die Architektur des Gesamtnetzwerks und dein persönlicher Zugang sind verschiedene Prüfgegenstände.

3 Schlüssel und Wallets verstehen

3.1 Was eine Wallet speichert

Deine Bitcoin befinden sich nicht als Dateien in einem Hardwaregerät. Das Netzwerk führt ausgebbare Transaktionsausgänge. Die Wallet verwaltet Informationen, mit denen sie passende Ausgänge erkennt und deren Ausgabe vorbereitet oder signiert. Sie kann außerdem Namen, Notizen und Zuordnungen speichern, die außerhalb der Blockchain liegen.

Geht das Gerät verloren, ist der Zugriff nicht zwingend verloren. Eine passende Sicherung und die nötigen Wiederherstellungsangaben können den Zugang auf einem anderen kompatiblen Gerät rekonstruieren. Geht die einzige Sicherung zusammen mit dem Gerät verloren, gibt es dagegen normalerweise keine zentrale Stelle, die den Schlüssel neu ausstellt.

Eine Wallet ohne eigene Schlüssel kann trotzdem Beträge und Adressen anzeigen. Diese Watch-only-Funktion ist nützlich, aber nicht bedeutungslos für die Privatsphäre. Wer ihre öffentlichen Ableitungsdaten kennt, kann unter Umständen viele zusammengehörige Vorgänge verfolgen.

3.2 Private Schlüssel und Signaturen unterscheiden

Ein privater Schlüssel ermöglicht passende digitale Signaturen. Eine Signatur bindet eine Autorisierung an bestimmte Daten. Sie ist keine Verschlüsselung der gesamten Transaktion. Öffentliche Transaktionsdaten bleiben grundsätzlich öffentlich auswertbar.

Aus einem privaten Schlüssel lässt sich der zugehörige öffentliche Schlüssel ableiten. Die umgekehrte Berechnung gilt mit heutigen praktikablen Verfahren bei korrekt erzeugten Schlüsseln als nicht durchführbar. Diese Aussage hängt von verwendeten Verfahren und Annahmen ab; sie sollte nicht als zeitloser Beweis absoluter Unangreifbarkeit formuliert werden.

Die häufigeren Alltagsrisiken liegen nicht in einer vollständigen mathematischen Rückrechnung. Phishing, schwache Zufallsquellen, kompromittierte Software und freiwillig herausgegebene Backups sind wesentlich näher am üblichen Bedienablauf. Deshalb konzentriert sich dein Schutz zuerst auf Erzeugung, Eingabe und Bestätigung.

3.3 Adressen als Ausgabebedingungen lesen

Eine Bitcoin-Adresse beschreibt in kompakter Form, wie ein neuer Ausgang gesperrt werden soll. Je nach Adresstyp werden unterschiedliche Skriptbedingungen verwendet. Eine Adresse ist nicht schlicht mit einem öffentlichen Schlüssel gleichzusetzen.

Die Wallet kann für neue Eingänge neue Adressen erzeugen. Das vermeidet bestimmte direkte Verknüpfungen, macht deine Nutzung aber nicht automatisch anonym. Gemeinsame Ausgaben, Abfragen an fremde Server und Zuordnungen bei Dienstleistern können Beziehungen weiterhin sichtbar machen.

Verwende die Empfangsfunktion deiner Wallet und vergleiche die vollständige Adresse auf dem unabhängigen Display des Signiergeräts, sofern dein Gerät diese Funktion bietet. Ein QR-Code spart Tipparbeit, ersetzt aber keine inhaltliche Prüfung. Ein manipuliertes Programm kann auch einen manipulierten QR-Code anzeigen.

3.4 Hierarchische Ableitung nachvollziehen

HD-Wallets leiten viele Schlüssel aus einem Ausgangsgeheimnis ab. BIP32 definiert dafür einen hierarchischen Aufbau mit erweiterten Schlüsseln. Das erleichtert Sicherung und Organisation, erzeugt aber zugleich wertvolle Metadaten. Ein erweiterter öffentlicher Schlüssel kann zur Beobachtung eines ganzen Zweigs reichen. [D09]

Der Ableitungspfad bezeichnet einen Weg in diesem Baum. Netzwerk, Kontonummer und Skripttyp beeinflussen, welche Adressen ein Programm findet. Zwei Programme mit denselben Wiederherstellungswörtern können deshalb zunächst unterschiedliche Konten anzeigen, ohne dass eine der Sicherungen falsch sein muss.

BIP84 beschreibt eine verbreitete Ableitung für native Segwit-Einzelunterschriften. Sie ist ein Beispiel für eine konkrete Konvention, keine universelle Regel für alle Wallets. Notiere den tatsächlich verwendeten Standard und Kontotyp in deiner Wiederherstellungsanleitung. [D11]

3.5 Drei Arten von Sicherung auseinanderhalten

Eine geheime Sicherung ermöglicht die Rekonstruktion von Schlüsseln. Eine Wallet-Datei kann zusätzlich Verschlüsselung, öffentliche Schlüssel, Notizen und Programmeinstellungen enthalten. Eine Betriebsdokumentation erklärt schließlich, welches Netzwerk, welcher Kontotyp und welches Verfahren benutzt wurden. Diese Informationen ergänzen einander.

Ein regelmäßiges Backup der Rechnerdatei ersetzt nicht die Prüfung der geheimen Wiederherstellung. Umgekehrt rettet eine Wortliste nicht automatisch selbst angelegte Etiketten oder die Buchhaltung. Bei Multisig sind außerdem die gemeinsam verwendete Ausgaberegel und die öffentlichen Daten der beteiligten Schlüssel wichtig.

Lege deshalb getrennte Aufbewahrungsregeln fest. Geheime Wiederherstellungsdaten gehören in einen besonders geschützten Bereich. Ein Geräteverzeichnis ohne Geheimnisse darf leichter zugänglich sein. Öffentliche Wallet-Daten sind nicht geheim wie ein Seed, aber sensibel genug, um sie nicht sorglos in eine allgemeine Cloud zu legen.

3.6 Öffentliche Ableitungsdaten bewusst exportieren

Ein Export für eine Beobachtungswallet sollte nur die benötigten öffentlichen Daten enthalten. Prüfe die gewählte Exportart und verwende zunächst eine Übungs-Wallet. Ein Dateiname mit Watch-only ist ein Hinweis, aber kein Ersatz für die Prüfung der tatsächlich enthaltenen Felder.

Notiere, welcher Empfänger die Datei erhalten hat. Ein später gelöschter eigener Export nimmt eine bereits kopierte Datei nicht zurück. Wenn dadurch eine umfassende Beobachtung möglich wurde, kann die Privatsphäre des bisherigen Kontos nicht allein durch ein neues Dateipasswort wiederhergestellt werden.

4 Wiederherstellungswörter und Passphrasen sichern

4.1 Das Sicherungsformat zuerst feststellen

Nicht jede Wortliste folgt demselben Standard. BIP39 beschreibt die Darstellung von Entropie mit Prüfsumme in einer geordneten Folge von Wörtern und die Ableitung eines Seeds. Gebräuchlich sind zwölf oder 24 Wörter; der Standard erlaubt weitere definierte Längen. Eine beliebige selbst erfundene Wortfolge ist keine gleichwertige Alternative. [D10]

Andere Systeme verwenden etwa SLIP39. Dabei können Sicherungen aus einzelnen Anteilen oder Schwellenkombinationen bestehen. Die Wortlisten und der Wiederherstellungsprozess unterscheiden sich von BIP39. Trezor beschreibt aktuell unter anderem 20-Wort-Sicherungen und nennt die jeweils unterstützten Geräte und Firmwarestände. Die Aussage, jede Hardware-Wallet habe immer 24 Wiederherstellungswörter, ist deshalb falsch. [D21, D22]

Notiere das Format, bevor du über ein Ersatzgerät entscheidest. Eine Funktion mit dem Namen Import kann private Schlüssel, eine BIP39-Wortfolge, einen Descriptor oder eine bestimmte Gerätedatei erwarten. Der gemeinsame Begriff Wallet garantiert keine Austauschbarkeit.

4.2 Ein neues Geheimnis korrekt erzeugen

Erzeuge eine produktive Sicherung mit der vorgesehenen Funktion eines überprüften Geräts oder einer geeigneten Wallet. Übernimm keine bereits ausgefüllte Karte aus einer Verpackung. Auch ein als Geschenk geliefertes Gerät mit einer vorbereiteten Wortliste ist kein vertrauenswürdiger Ausgangspunkt.

Wähle Wörter nicht selbst aus einem Buch oder nach Erinnerungen. Menschen erzeugen typischerweise keine gleichmäßig verteilten Zufallswerte. Die Stärke einer Sicherung hängt wesentlich von ihrer Entstehung ab. Eine lange, aber vorhersehbare Folge kann deutlich schlechter sein als eine korrekt erzeugte kürzere Standardfolge.

Während der Einrichtung bleiben Kameras und Bildschirmaufnahmen ausgeschaltet. Schreibe Wörter in der angezeigten Reihenfolge und nummeriere ihre Positionen. Vermeide Fotos, Kopien in einer Notiz-App und Eingaben in Webseiten. Ein normales Cloud-Backup des Telefons kann sonst unbemerkt eine zusätzliche Kopie erzeugen.

4.3 PIN und Passphrase nicht verwechseln

Die Geräte-PIN oder ein Gerätepasswort schützt den Zugang zu einem bestimmten Gerät. Sie ist normalerweise nicht Teil der blockchainseitigen Ausgabebedingung. Wer eine vollständige brauchbare Sicherung besitzt, kann die Wallet häufig auf einem anderen Gerät rekonstruieren, ohne die alte PIN zu kennen.

Eine zusätzliche BIP39-Passphrase fließt dagegen in die Ableitung ein. Mit derselben Wortfolge und einer anderen Passphrase entsteht eine andere Wallet. Ein Tippfehler kann daher zu einem vollständig leeren, technisch gültigen Konto führen, statt eine verständliche Fehlermeldung auszulösen.

Die Bezeichnung „25. Wort“ ist missverständlich. Die Passphrase muss nicht ein Wort aus der Sicherungsliste sein und ist nicht bloß eine weitere Prüfstelle. Länge, Zeichensatz, exakte Schreibweise und Eingabemethode müssen mit dem verwendeten Gerät zusammenpassen. Prüfe die dokumentierte Unterstützung, bevor du dieses zusätzliche Geheimnis verwendest.